Partial Model Checking and Partial Model Synthesis in LTL using a Tableau-Based Approach

Serenella Cerrito, Valentin Goranko, and Sophie Pinchinat

(FSCD 2023, LIPICS)

Transition system, partially given:

a) truth values of some propositions in some states are partially known (only)

b) not all transitions between given states are known

c) not all states and their transitions are known.

Two natural questions:

i) Is there a way to extend a partially constructed transition system such that a property η holds? ("Partial model synthesis")

ii) Does the known part of the system suffice to verify η, no matter how the partial information might be extended (completed)?

Partial transition system (PTS) $\mathcal{M} = \langle S, A, \xrightarrow{}_{must}, \xrightarrow{}_{may}, I, AP, L\rangle$ (known transitions; possible, not yet determined transitions)

where $\xrightarrow{}_{must} \subseteq \xrightarrow{}_{may} \subseteq S \times A \times S$

$\mathcal{M}$ is transition-complete if $\xrightarrow{}_{may} = \xrightarrow{}_{must}$ (corresponds to a TS (non-partial))

$L : S \to 3^{AP}$ labeling function

$3 = \{0, 1, ?\}$ (false $\bot$, true, don't know)

PTS $\mathcal{M}$ is complete if $\mathcal{M}$ is transition-complete and L assigns only values in $\{0,1\}$ but no "?"s (i.e. $L : S \to 2^{AP}$)

Let $\mathcal{M} = \langle S, A, \xrightarrow{}_{must}, \xrightarrow{}_{may}, I, AP, L\rangle$ a PTS and $L' : S \to 3^{AP}$

We say L' is extension of L ($L \preceq L'$) if, for all $s \in S$, $L(s,p) \neq$ "?", then $L'(s,p) = L(s,p)$ for $p \in AP$

L' is a complete extension of L ($L \preceq^c L'$) (completion) if L' is an extension of L and $L' : S \to 2^{AP}$ (L' does not have "?" as values)

Let $\mathcal{M} = \langle S, A, \xrightarrow{}_{must}, \xrightarrow{}_{may}, I, AP, L\rangle$ and $\mathcal{M}' = \langle S', A, \xrightarrow{}'_{must}, \xrightarrow{}'_{may}, I, AP, L'\rangle$ be PTSs.

We say $\mathcal{M}'$ is extension of $\mathcal{M}$ if: $S \subseteq S'$, $\xrightarrow{}_{must} \subseteq \xrightarrow{}'_{must}$, $\xrightarrow{}'_{may} \subseteq \xrightarrow{}_{may}$, $L \preceq L'$

if $\xrightarrow{}'_{may}$ is serial, then $\mathcal{M}'$ is a total extension of $\mathcal{M}$. $\xrightarrow{}'_{may} \cap (S \times A \times S) \subseteq \xrightarrow{}_{may}$

We say that $\mathcal{M}'$ is a completion of $\mathcal{M}$ ($\mathcal{M} \preceq^c \mathcal{M}'$) if:

$S \subseteq S'$, $\xrightarrow{}_{must} \subseteq \xrightarrow{}'_{must} = \xrightarrow{}'_{may} \subseteq \xrightarrow{}_{may}$, $L \preceq^c L'$

and $\mathcal{M}'$ is serial.

$\xrightarrow{}_{must} \subseteq \xrightarrow{}'_{must} \cap (S \times A \times S) = \xrightarrow{}'_{may} \cap (S \times A \times S) \subseteq \xrightarrow{}_{may}$

(2) 4 Extension Problems (Model Checking Problems)

concerning a partial TS $\mathcal{M}$ and an LTL-formula η and a state s_0 of $\mathcal{M}$

EE: Existential extension for path existence
Are there a total extension $\mathcal{M}'$ of $\mathcal{M}$ and a path $\pi = s_0 s_1 s_2 \ldots$ in $\mathcal{M}'$ such that $\text{trace}(\pi) \models \eta$? $\quad (\exists\, \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \wedge \exists \pi \text{ path in } \mathcal{M}' \text{ from } s_0 : \pi \models \eta$

EA: Existential extension for all paths
Is there a total extension $\mathcal{M}'$ of $\mathcal{M}$ so that for all paths $\pi = s_0 s_1 s_2 \ldots$ in $\mathcal{M}'$, $\text{trace}(\pi) \models \eta$? $\quad (\exists \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \wedge \forall \pi \text{ from } s_0 : \pi \models$

AE: Universal extension for path existence
Do for all total extensions $\mathcal{M}'$ of $\mathcal{M}$ exist a path $\pi = s_0 s_1 s_2 \ldots$ such that $\text{trace}(\pi) \models \eta$? $\quad (\forall \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \to \exists \pi \text{ from } s_0 : \pi \models \eta)$?

AA: Universal extension for all paths
Do for all total extensions $\mathcal{M}'$ of $\mathcal{M}$ and for all paths $\pi = s_0 s_1 s_2 \ldots$ in $\mathcal{M}'$, is hold that $\text{trace}(\pi) \models \eta$?

$(\forall \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \to \forall \pi \text{ from } s_0 : \pi \models \eta)$?

General observations:

[01] EE and AA are dual: $\quad \langle \mathcal{M}, s_0, \eta \rangle \in EE \iff \langle \mathcal{M}, s_0, \neg\eta \rangle \notin AA$ (1)
$\langle \mathcal{M}, s_0, \neg\eta \rangle \notin EE \iff \langle \mathcal{M}, s_0, \eta \rangle \in AA$

[02] EA and AE are dual: $\quad \langle \mathcal{M}, s_0, \eta \rangle \in EA \iff \langle \mathcal{M}, s_0, \neg\eta \rangle \notin AE$ (2)
$\langle \mathcal{M}, s_0 \neg\eta \rangle \notin EA \iff \langle \mathcal{M}, s_0, \eta \rangle \in AE$

(1): $\langle \mathcal{M}, s_0, \eta \rangle \in EE \iff \exists \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \wedge \exists \pi \text{ path in } \mathcal{M}' \text{ from } s_0 : \pi \models \eta)$
$\iff \exists \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \wedge \exists \pi \text{ path in } \mathcal{M}' \text{ from } s_0 : \pi \not\models \neg\eta)$
$\iff \exists \mathcal{M} (\mathcal{M} \preceq^c \mathcal{M}' \wedge \neg \forall \pi \text{ path in } \mathcal{M}' \text{ from } s_0 : \pi \models \neg\eta)$
$\iff \neg \forall \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \to \forall \pi \text{ path in } \mathcal{M}' \text{ from } s_0 : \pi \not\models \neg\eta)$
$\iff \langle \mathcal{M}, s_0, \neg\eta \rangle \notin AA$

(2): $\langle \mathcal{M}, s_0, \eta \rangle \in EA \iff \exists \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \wedge \forall \pi \text{ in } \mathcal{M}' \text{ from } s_0 : \pi \models \eta)$
$\iff \exists \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \wedge \forall \pi \text{ in } \mathcal{M}' \text{ from } s_0 : \pi \not\models \neg\eta)$
$\iff \exists \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \wedge \neg \exists \pi \text{ in } \mathcal{M}' \text{ from } s_0 : \pi \models \neg\eta)$
$\iff \neg \forall \mathcal{M}' (\mathcal{M} \preceq^c \mathcal{M}' \to \exists \pi \text{ in } \mathcal{M}' \text{ from } s_0 : \pi \models \neg\eta)$
$\iff \langle \mathcal{M}', s_0, \neg\eta \rangle \notin AE$

$\langle \{s_0\}, A, \Phi, \{s_0\} \times A \times \{s_0\}, s_0, AP, L \rangle$ = $\mathcal{M}$ completely unknown

[03] $\mathcal{M}$ completely unknown $\Rightarrow$
$(\langle \mathcal{M}, s_0, \eta \rangle \in EE \iff \eta \text{ is satisfiable})$
$(\langle \mathcal{M}, s_0, \eta \rangle \in EA \iff \eta \text{ is satisfiable})$
$\Rightarrow (\langle \mathcal{M}, s_0, \eta \rangle \in AA \iff \eta \text{ is valid})$
$\wedge (\langle \mathcal{M}, s_0, \eta \rangle \in AE \iff \eta \text{ is valid})$

[04] $\mathcal{M}$ is complete $\Rightarrow$
$\{\langle \mathcal{M}, s_0, \eta \rangle \in EE\}$ … existential (path) model checking problem
$\langle \mathcal{M}, s_0, \eta \rangle \in AE\}$
$\{\langle \mathcal{M}, s_0, \eta \rangle \in EA\}$ … universal (path) model checking problem
$\langle \mathcal{M}, s_0, \eta \rangle \in AA\}$

...nd 4: Extension Problems (Model Synthesis Problems)

EE^S: Given $\langle M, s_0, \eta \rangle$ (partial transition system / CTL-formula / state) — construct →
- M' such that $M \trianglelefteq^c M'$ and π path in M' with $\pi \models_{M'} \eta$, $\pi = s_0 s_1 s_2 \ldots$
- answer "such a model does not exist"

EA^S: Given $\langle M, s_0, \eta \rangle$ — cons →
- M' with $M \trianglelefteq^c M'$ such that $s_0 \models_{M'} \eta$
- answer "such a completion of M does not exist"

---

3 subkinds of extension problems:

(i) **label extension**: states and transitions are fixed, labels of states / interpretation function needs to be extended

(ii) **transition extension**: states and labels are fixed, but new transitions are added

(iii) **state extension**: where new states with partial or complete label as well as transitions to and from them can be added.

Contribution of the paper:

1) Complexity results for all extension problems, based on brute-force exploration: all problems are PSPACE-complete just like Existential (Path) Model Checking and Universal (Path) Model Checking

2) Use of tableau methods to obtain "minimal" complete extensions thus use constructive rather than brute-force exploration.
- based on tableau methods for solving LTL-satisfiability (Wolper, Gorankо).

Step 1: Solution of EE for Label-extension subproblem by tableau metho
(core) (and dually for AA)

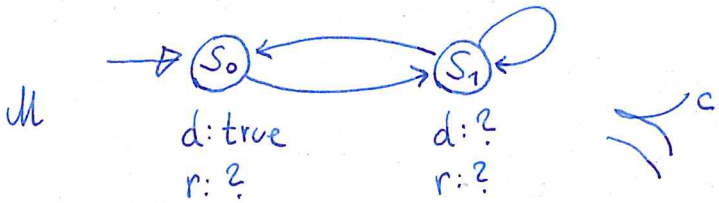
Step 2: Adaptation of this solution to transition-extension and state-extension problem versio

Step 3: Transfer of solution methods to problems EA and AE.

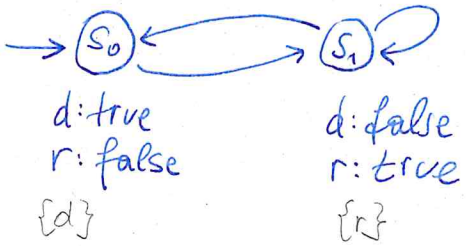
Example. Automatic subway

"the doors cannot be open while the train is running, and the train will eventually run"

$\eta_0 := \Box(r \to \neg d) \wedge \Diamond r$



positive intended result of EE^S for $\langle \mathcal{M}, s_0, \eta \rangle$



Completion of $\mathcal{M}$

LTL-syntax in the paper: $\bigcirc\Phi$ $\Box\Phi$

$\Phi ::= \top \mid \bot \mid p \mid \neg\Phi \mid \Phi \wedge \Phi \mid X\Phi \mid G\Phi \mid \Phi U \Phi$

$\vee, \to, \leftrightarrow, F$ defined $\Diamond$

$F\Phi := \neg G \neg \Phi$

$\Diamond\Phi$

formulas	Conjunctive components
$\neg\neg\Phi$	Φ
$\Phi \wedge \Psi$	Φ, Ψ
$\neg(\Phi \vee \Psi)$	$\neg\Phi, \neg\Psi$
$\neg(\Phi \to \Psi)$	$\Phi, \neg\Psi$
$\Box\Phi$	$\Phi, \bigcirc\Box\Phi$
$\neg\Diamond\Phi$	$\neg\Phi, \bigcirc\neg\Diamond\Phi$
$\neg(\Psi U \Phi)$	$\neg\Psi \vee \bigcirc\neg(\Psi U \Phi), \neg\varphi$

e.g. $\Box\Phi \equiv \Phi \wedge \bigcirc\Box\Phi$

formulas	disjunctive Component
$\Phi \vee \Psi$	Φ, Ψ
$\Phi \to \Psi$	$\neg\Phi, \Psi$
$\neg(\Phi \wedge \Psi)$	$\neg\Phi, \neg\Psi$
$\Diamond\Phi$	$\Phi, \bigcirc\Diamond\Phi$
$\Psi U \Phi$	$\Phi, \Psi \wedge \bigcirc(\Psi U \varphi)$
$\neg\Box\Phi$	$\neg\Phi, \bigcirc\neg\Box\Phi$

e.g. $\Diamond\Phi \equiv \Phi \vee \bigcirc\Diamond\Phi$

formulas	Successor Compone
$\bigcirc\varphi$	φ
$\neg\bigcirc\varphi$	$\neg\varphi$

Extended closure of a formula Φ

$ecl(\Phi)$ is the least set of formulas such that:

1. $\Phi \in ecl(\Phi)$
2. $ecl(\Phi)$ is closed under taking all conjunctive, disjunctive, successor components of formulas in $ecl(\Phi)$.

$ecl(\Gamma) := \bigcup \{ecl(\Phi) / \Phi \in \Gamma\}$

A set Γ of formulas is closed if $\Gamma = ecl(\Gamma)$.

Γ is "patently inconsistent" if it contains $\bot$, $\neg\top$, or a contradictory pair of formulas Φ and $\neg\Phi$

Γ is "fully expanded" if:

1. Γ is not patently inconsistent
2. for every conjunctive formula in Γ, all of its conjunctive components are in Γ
3. for every disjunctive formula in Γ, at least one of its disjunctive components is in Γ.

Γ is a full expansion of a set Δ of formulas if Γ results by repeated applications of the following rules, where initially no formula is marked as "used":

(C-Comp) for every conjunctive formula φ in the current set Δ that has not been marked as "used", add all conjunctive components of φ.

(D-Comp) for every disjunctive formula φ in the current set Δ that has not been marked as "used", add one of its disjunctive components to Γ and mark φ as "used".

A Hintikka trace (HT) for a closed set Γ of formulas is a mapping $H: \mathbb{N} \to \mathcal{P}(\Gamma)$ satisfying the following conditions for every $u \in \mathbb{N}$:

1. $H(u)$ is fully expanded
2. $\Phi \in H(u)$ is a successor formula $\Rightarrow$ $scomp(\Phi) \in H(u+1)$ (successor component of Φ)
3. If $\Psi \cup \Phi \in H(u)$, then there exists $i \geq n$ such that $\Phi \in H(u+i)$ and $\Psi \in H(u+j)$ for all j such that $0 \leq j < i$.

Φ is satisfiable in a Hintikka trace H if $\Phi \in H(u)$ for some $u \in \mathbb{N}$.

Thm. An LTL formula η is satisfiable $\Leftrightarrow$ η is satisfiable in some Hintikka trace